International Journal of Computer Networking,
Wireless and Mobile Communications (IJCNWMC)
ISSN (P): 2250-1568; ISSN (E): 2278-9448
Vol. 7, Issue 2, Apr 2017, 23-32

BAYESIAN BELIEF NETWORKS (BBN) BASED RISK ASSESSMENT FOR DEPLOYED C4I SYSTEM

MANOJ TYAGI, SHIPRA RAHUL & ANOOP KUMAR RAI

Central Research Laboratory, Bharat Electronics Ltd, Ghaziabad, Uttar Pradesh, India

ABSTRACT

Bayesian Belief Network (BBN) is a popular means of representing uncertainty within various problem domains. It facilitates the graphical representation of complex problems and allows analyst to make predictions on the likelihood of a hypothesis, given incomplete information. Risk assessment for deployed C4I system, is one such area where BBNs intuitively fits in. In this paper, BBNs were constructed using NETICA tool to reflect a wide spectrum of potential risks to the deployed C4I system with a view to assess system's risks against combinatorial scenarios in which risks may manifest themselves. Different BBN sub-models for each kind of risks were developed and later integrated into main model. Each risk, thus, was modeled in significant detail. However, the cross linkages between risk sub- models were realized only in the main integrated model. Major emphasis was given to risks at physical, environmental, hardware, software, and network level. The risk scenarios ranged from accidental or inadvertent to being initiated by enemy actions both external as well as internal. The inputs required by the models can be either summaries from statistical data or based on expert judgments, as required or if statistical data is unavailable.

KEYWORDS: Bayesian Belief Networks, Risk Assessment, C4I, CPT

Received: Feb 04, 2017; **Accepted**: Mar 27, 2017; **Published:** Apr 01, 2017; **Paper Id**.: IJCNWMCAPR20173

Original Article

INTRODUCTION

Command, Control, Communication, Computers and Intelligence (C4I) systems provide battlefield information for commanders to make decisions and control military forces to accomplish missions.[1] C4I system provides comprehensive information to the commanders in a timely fashion and enables them to disseminate orders expeditiously. A component system can be C4I system, weapon system, logistic system or an IT system. Along with these, software and database resources are the most important resources to C4I system. These include source programs and communication programs along with entire data that is either in transit over communication media, during execution, stored on-line, archived off-line, backups or audit logs. The information assets are at risk from potential risks such as user errors, accidents, long-term system failures, natural disasters, and criminal or malicious action undertaken by 'insiders' as well as our enemies. Such events could result in irrevocable damage or loss of information resources, loss of data integrity, or unacceptable interruptions in normal data processing activities and may also result a break in data flow over the network. Thus, risk assessment of such a system assumes importance [2].One major problem while assessing risks of such a system is that, the available data or information required for the purpose is often incomplete and is uncertain.

Bayesian Belief Networks (BBNs) based NETICA tool is, now-a-days, becoming a popular tool to support decision-making processes as they can be used to generate optimal predictions/decision even when key pieces of information are missing. This paper, however, attempts not suggest any modification or a change to the

existing policies. The paper aims at applying Bayesian Belief Network approach to model various risks and assessment for a given deployed C4I system.

BAYESIAN BELIEF NETWORKS (BBN)

A Bayesian Network models a problem by mapping out cause-and-effect relationships among key variables and assigning to them probabilities that represent the extent to which one variable is likely to affect another [3]. A chance node (or simple a node) in a BBN takes up multiple discrete states and refers to a variable in the problem domain. The conditional probability table defines the probability of the node taking a particular state given its parent node(s) state. The essence of the Bayesian approach is to provide a mathematical rule explaining how you should change your existing beliefs in the light of new evidence. It allows scientists to combine new data with their existing knowledge or expertise. Bayesian Statistics deals with the concept of Subjective Probability. [4] The structure of a BBN readily permits the fusion of expert domain knowledge with an information stream, and the updating of beliefs as new information or evidence is obtained. When we enter evidence in form of observations on other nodes in the system, the BBN efficiently propagates this evidence to whichever other nodes in the network are affected by it and updates probability distributions at those nodes given the new evidence.

MAJOR RISKS FOR DEPLOYED C4I SYSTEM

Confidentiality, authentication, data integrity and non-repudiation of the information are the main assets for deployed C4I systems. Information systems have long been at risk from malicious actions or inadvertent user errors and from natural and man-made disasters. A principal challenge many agencies face in this scenario is in identifying and ranking the information security risks to their operations, which is the first step in developing and managing an effective security program. Taking this step helps ensure that organizations identify the most significant risks and determine what actions are appropriate to mitigate them.[6] The possible risks to any C4I systems network, apart from natural disasters, may range from overall network slowdown & unavailable services to malicious unauthorized access to classified information. These risks may be categorized as: physical, personal security, procedural control, environmental, manmade, documentation, hardware, software, database and network. Risk assessment of deployed C4I system is the determination of quantitative or qualitative estimate of identified risks related to a well defined situation and a recognized risk.

CONSTRUCTION OF THE BBN

There are two main approach for the construction of BBN, first is Qualitative and the second is quantitative. This paper presents use of NETICA for construction of both approaches.

NETICA is a powerful, easy to use, complete program for working with belief networks and influence diagrams. It has smooth user interface for drawing the networks and relationships between variables may be entered as individual probabilities, in the form of equations or learned from data files. NETICA tool is used for automated diagnosis, prediction, financial risk management, portfolio allocation, modeling ecosystem, sensor fusion etc. one can first focus on specifying the qualitative structure of the domain and then focus on quantifying the influences. There is root node (parent) and Leaf node (child), Leaf nodes are the ones which have outgoing arrow that shows dependency on other nodes. Leaf node has a local probability distribution table for the initial belief. Root node is the one which have incoming arrows that shows dependency of other nodes to parent node. For root nodes the joint probability distribution table requires a number of values exponential in the number of variables. [5]

- **Capturing Qualitative Aspect**

Qualitative Probabilistic Network (QPN) have been put forward as qualitative analogues to Bayesian networks, and allow modeling interaction in terms of qualitative signs. The separation of qualitative representation and the numeric quantification of the influences between variables have a significant advantage for knowledge engineering. In results model is guaranteed to have a complete specification of the joint probability distribution. [10]

Figure 1 is showing the top level view of the major risks in C4I deployed system. Subsequently, each risk is then modeled in detail.

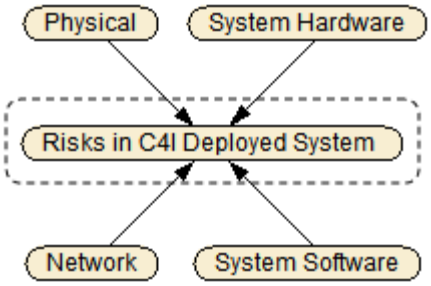


Figure 1: Top Level C4I System Risks Domain Variable

Major risks in C4I deployed system are Physical, System Hardware, Network, System software related. Physical security is the protection of physical equipments from damage by natural disaster and intruders.

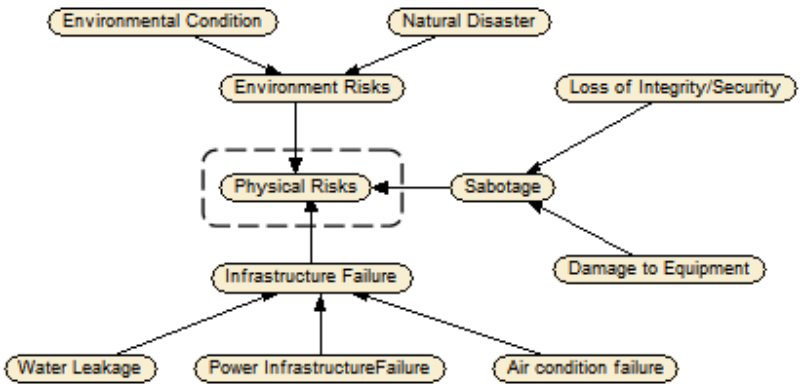


Figure 2: Physical Risks Sub-Model

To make C4I systems less vulnerable to physical risk (evidently from figure 2), appropriate measures for the prevention, detection, early warning of, and recovery from emergency conditions must be considered to prevent physical breach in security. Figure 2 shows the Physical risk sub model which includes main factors like environment risk, sabotage, infrastructure risks.

Hardware resources are at risk if they are not protected by security agencies at their installed sites. These resources are distributed over a wide geographical area. Main risk for system hardware is Enemy direct attack and hardware intrusion by these tactics enemy can destroy the resources. Figure 3 shows system hardware risks factors.

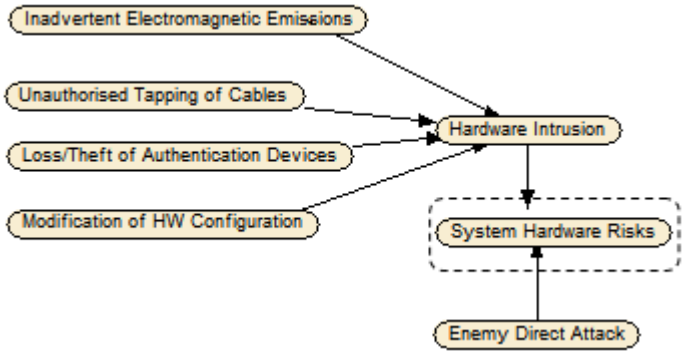


Figure 3: System H/W Risks Sub-Model

System software and database risks may lead to compromise of sensitive, confidential data. The data could be accessed, manipulated, destroyed and malicious code introduced within the software that could lead to system data compromise. Unauthorized access to C4I systems is posed due to the operating system risks, database risks or the application software risks as shown in figure 4.

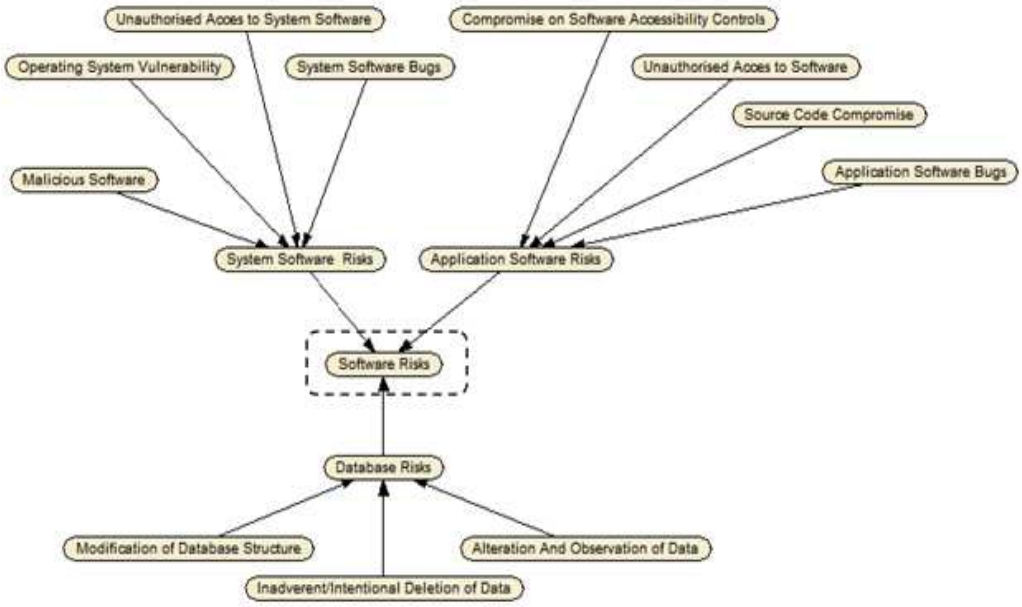


Figure 4: System Software & Database Risks Sub-Model

Risks emanating as part of an intentional or unintentional network attack are quite possible on C4I system network. These risks need to be prevented in order to provide the system users the acceptable degree of assurance and availability of network services. The main factor constituting the network risks are shown in figure 5.

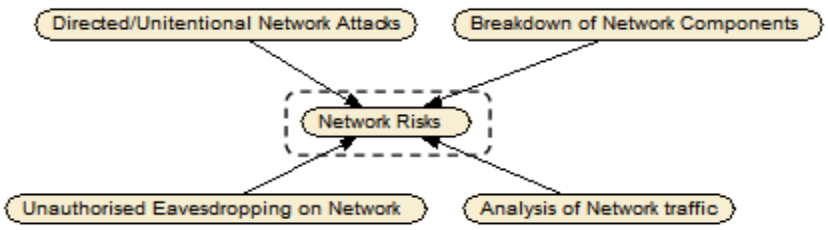


Figure 5: Network Risks Sub-Model

Main factors to assess the risk of C4I deployed system's Network are Directed/Unintentional Network Attacks, Breakdown of Network Components, Unauthorized Eavesdropping on Network, Network traffic. Risk analysis of a given deployed C4I system capture the qualitative aspect of the factors influencing the vulnerability. Next step in the construction of BBNs is to quantify the experts' knowledge in term of probability distributions. Next section illustrates the knowledge elicitation and representation for BBNs. [7]

- **Capturing quantitative Aspect**

For a BBN There are two possible sources of probability distributions – expert knowledge or data sets and their relationship. In the quantitative approach BBN includes definition of joint probability distributions to reflect all the possible combinations of states of nodes in the network. According to studies people are better at estimating probabilities in the forward direction. The causal relationship represented by the arcs in the DAG also assists experts in determining probabilities. The expert has to think about the probability distribution of one variable at a time considering the probability distributions of its parent node(s) and the conditioning events as fixed scenarios. For example, in figure 6, while giving the probability distributions of "Network risk" the expert has to consider "Directed/unintentional Network attack", "Breakdown of Network components", "Unauthorized Eavesdropping on network", "Analysis of network traffic" probability distributions influencing the states of "Network risk" node as shown in figure 6.

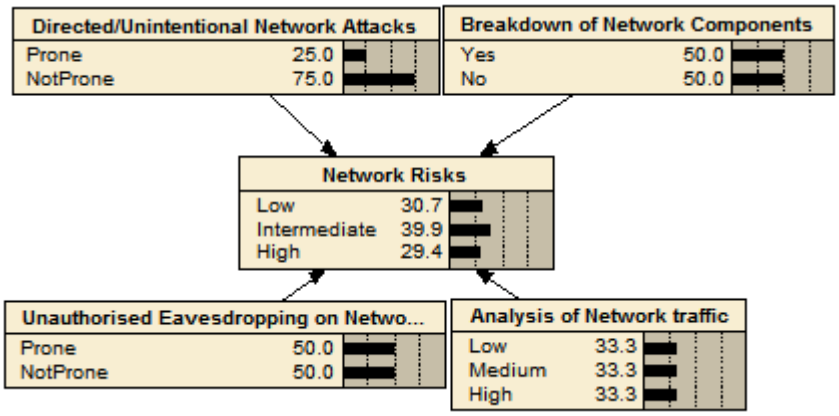
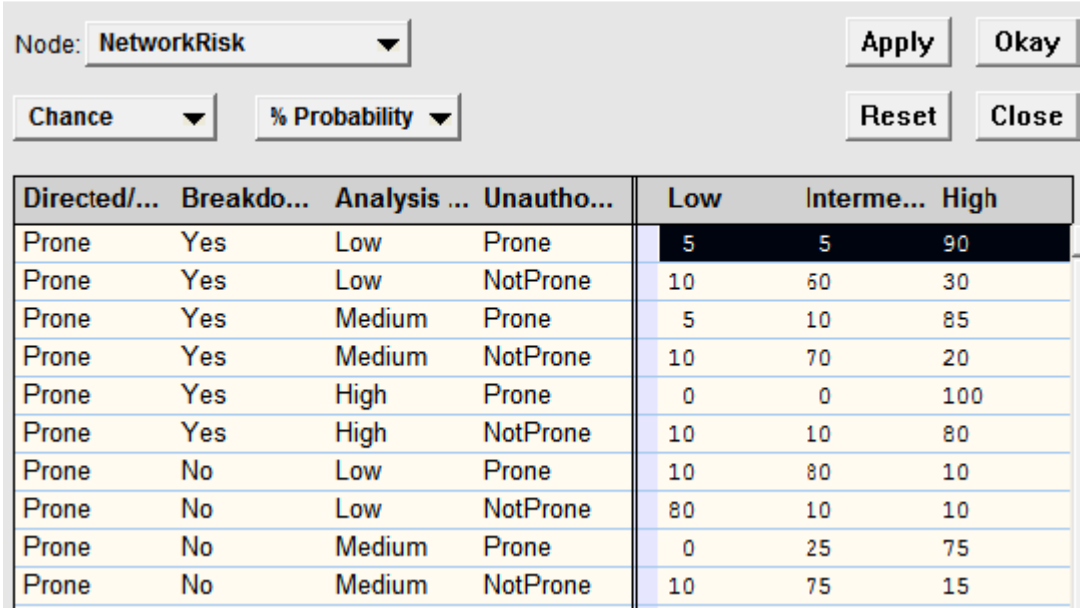


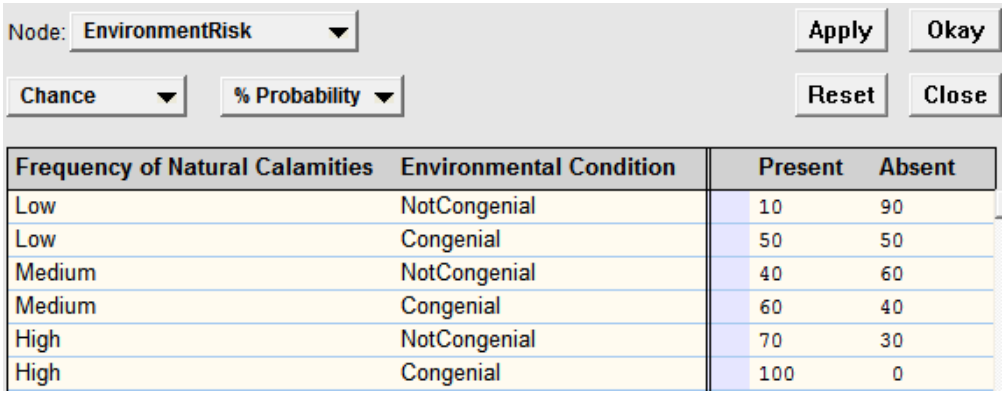
Figure 6: System Hardware Risks Sub-Model

Initially, a network is roughly quantified. Sensitivity analysis is then used to identify which variables have the most impact on the network output. The probabilities for these influential variables are then replaced with more precise estimates from the experts. This approach, thus, reduces the quantification burden placed upon the expert. The BBN for this paper are illustrative only and have been built using probabilities derived from the authors, although it would be possible to study a given C4I deployed system in detail to determine quantifications with the help of domain experts. Following tables give a glimpse of the quantification process using NETICA (BBN software from Norsys Corp.) probability distribution tables.[8]



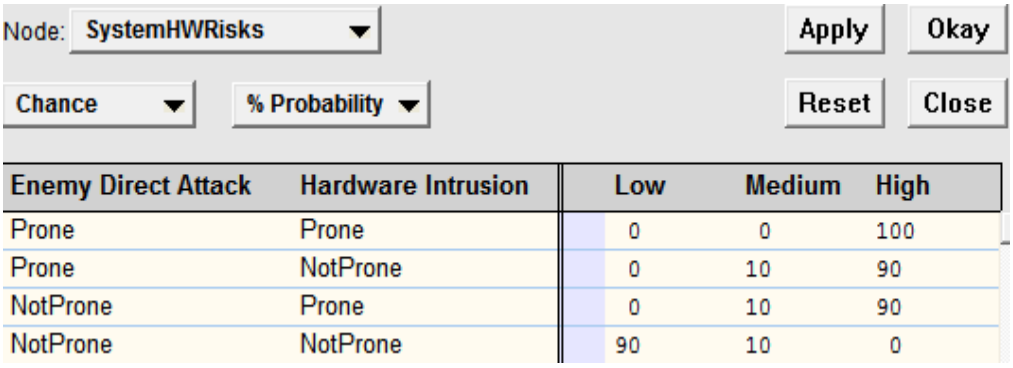
Directed/...	Breakdo...	Analysis ...	Unautho...	Low	Interme...	High
Prone	Yes	Low	Prone	5	5	90
Prone	Yes	Low	NotProne	10	60	30
Prone	Yes	Medium	Prone	5	10	85
Prone	Yes	Medium	NotProne	10	70	20
Prone	Yes	High	Prone	0	0	100
Prone	Yes	High	NotProne	10	10	80
Prone	No	Low	Prone	10	80	10
Prone	No	Low	NotProne	80	10	10
Prone	No	Medium	Prone	0	25	75
Prone	No	Medium	NotProne	10	75	15

Figure 7



Frequency of Natural Calamities	Environmental Condition	Present	Absent
Low	NotCongenial	10	90
Low	Congenial	50	50
Medium	NotCongenial	40	60
Medium	Congenial	60	40
High	NotCongenial	70	30
High	Congenial	100	0

Figure 8



Enemy Direct Attack	Hardware Intrusion	Low	Medium	High
Prone	Prone	0	0	100
Prone	NotProne	0	10	90
NotProne	Prone	0	10	90
NotProne	NotProne	90	10	0

Figure 9: Conditional probability distribution tables

Conditional Probability Tables (CPT) in figure 9 are for “Network Risk” node in Network Risk sub-model (figure 2), “Environment Risk” node in Physical Risk sub-model (figure 3) and “System HW Risks” node in System hardware risk sub model respectively.

The CPT is simply a table that one probability for every possible combination of parent and child states. This is an N+1 dimensional table, where N is the number of parents.

Probability of each row must sum exactly 100. This is because each is summarizing the probabilities of one possible world, one where the parents are in the given states. [9]

The current implementation of BBNs for Risk analyses of Deployed C4I system had 39 nodes. The numbers of total states for Risk sub-models were 38 for physical, 15 for system hardware, 35 for system software, 11 for network and 4 states for the Risk node making up a total of 103 states. Without any organization, (as an exaggerated view) this would have amounted to astronomical 103 factorial rows of conditional probabilities distributed in 39 conditional probability tables. The benefit of describing the domain knowledge in BBNs is evident, as each of the 39 tables now only contains an average of only 8 conditional probability rows. Qualitative description led to 27 leaf nodes and 12 nodes which had parents. For each leaf node initial belief rows were reduced to only 58 (approx 2.5 on average). For conditional nodes as distributions were to be given only on the basis of immediate parent nodes, further reduced the number of rows drastically. Therefore, by using BBNs the representation of expert's knowledge about the complex domain of C4I deployed system was simplified to an enormous extent.

UTILITY OF CONSTRUCTED BBNS FOR RISK ANALYSES OF DEPLOYED C4I SYSTEM

Determination of the posterior probability of some random variables is the most common computation performed using Bayesian networks. Bayesian networks have considerable potential for use as tools to risk assessment. The key strength of such networks lies in the provision of a statistically coherent method for combining probabilities across a complex framework based on both belief and evidence. Because of the symmetric nature of conditional probability, this computation can be used to perform both diagnosis and prediction. Other common computations are: computing the probability of the conjunction of a set of random variables, computing the most likely combination of values of the random variables in the network, and computing the piece of evidence that most influenced or will have the most influence on a given hypothesis. Multiple risk scenarios can be envisaged by providing evidence on the concerned nodes and the affect can be observed on the risk variables and subsequently on the risks node. For instance, if the specified operational conditions water leakage are low then the belief of physical risk existence increase from High to medium as shown in the figure 10 (a) & (b) below.

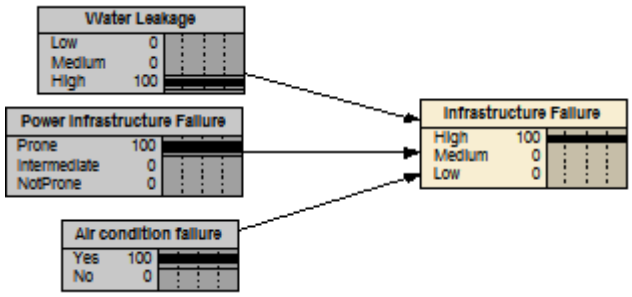


Figure 10a: Infrastructure Failure Posterior Probability Distribution for Evidences on Higher Side

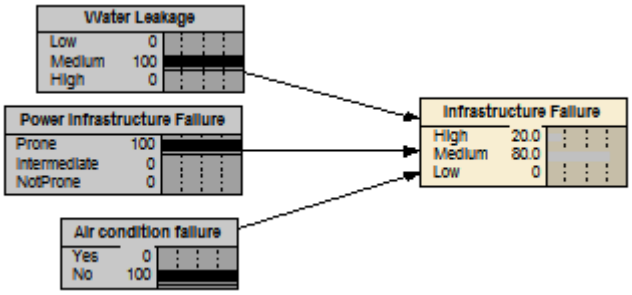


Figure 10b: Infrastructure Failure Posterior Probability Distribution for Evidences on Intermediate Side

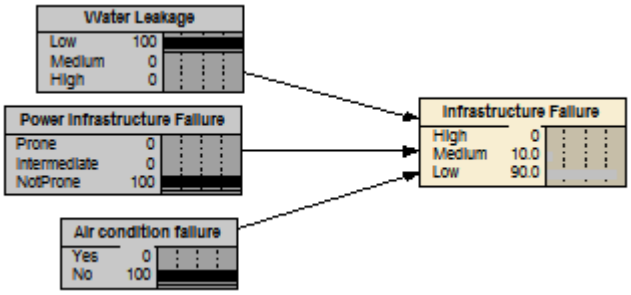


Figure 10c: Infrastructure Failure Posterior Probability Distribution for Evidences on Lower Side

There are a number of ways in which results from applying the Bayesian network to the risk assessment of C4I deployed system can be presented to the user. For Bayesian networks that compute the value of an attribute on nodes or links, a table may be displayed listing each node or link, and the new attribute. The columns in this table may be sorted, so the user can easily determine who among the individuals has the highest or lowest values for a particular attribute. In addition to the attribute value itself, the BBN provides a degree of certainty with the answer. It supports this by also associating an uncertainty value with the attribute. There is still, as always, a considerable scope for improvement for constructed BBNs in terms of addition of new factors and expansion of sub-factors. One such influencing node could have been the amount of redundancy provided at hardware and networking assets level. This node may have helped in neutralizing some inadvertent risks by improving the 'up-time'. Additionally, since assets of most of the C4I deployed Systems in place are geographically displaced, the effect of local factors may assume higher importance than the usual generic ones. For instance, the operating limits (environmental) might become dominant in areas where there are sub-zero temperatures all round the year. The assets nearing border or line-of-control may be most prone to direct attack by enemy, other factor being less significant as compared to this.

CONCLUSIONS

It is very important to protect and secure the information flowing and hardware used on Deployed C4I system from all risks. The goal of the paper was to utilize Bayesian Belief Networks (BBNs) approach as a process for enhancing risk assessment of deployed C4I system and to demonstrate the effectiveness of this approach on an implemented system as network sub-models using NETICA tool. The concept of BBN was examined with reference to its applicability in risk analyses of deployed C4I system. Various risk models (BBNs) were developed to capture the qualitative domain knowledge for all the possible factors. Quantification process of the captured expert knowledge about deployed C4I system was discussed and the benefits of the approach established. Simple scenarios have taken to show the utility of BBNs in deployed C4I system risk assessment.

The user can perform risk assessment tasks with incomplete data, nodes with uncertain attributes, and inconclusive relationships in Bayesian belief networks sub models. Because of their attributes and relationships this model allows the user to infer new relationships between nodes that were not revealed in the original data, and to identify nodes in the network that are of particular interest. These capabilities make Bayesian belief networks a powerful tool in conducting risk assessment of C4I deployed system.

REFERENCES

1. *Alghamdi, A. S.,(2009). Evaluating Defense Architecture Frameworks for C4I System Using Analytic Hierarchy Process.*
2. *Information security assessment guidelines URL (2016) www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html*
3. *Korb, K.B., & Nicholson, A.E. (2003). Bayesian artificial intelligence, chapter 2 Introducing Bayesian networks. http://www.csse.monash.edu.au/bai*
4. *Kevin Murphy (1998). A brief introduction to graphical models and baysian networks. http://www.cs.ubc.ca/~murphyk/Bayes/bnintro.html*
5. *Belief network theory, URL(2000) www.csse.monash.edu.au/hons/projects/2000/Daniel.Willis/node5.html*
6. *National research council (1999). Realizing the potential of C4I:Fundamental challenges. https://www.nap.edu/read/6457/chapter/1*
7. *Stewart, G. B, Higgins, J. P. T, Schunemann, H.& Meader, N. (2015).The use of Bayesian networks to assess the quality of evidence from research synthesis.*
8. *Ni, Z., Phillips, L.D,& Hanna, G.B. (2011). Exploring Bayesian Belief Networks Using Netica.*
9. *Krieg, M.L.(2001)Tutorial on Bayesian belief networks.*
10. *Lucas, P.J.F. (2004). Bayesian network modeling through qualitative patterns.*